Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A system for generating and verifying signatures on hardcopy documents comprising:
a signor key associated with a signor of a hardcopy document;
document data required to be on the hardcopy document;
a signature generation part for generating a document signature using the signor key to encode data selected from the document data, and which is then associated with the hardcopy document;
a data indicator associated with the hardcopy document and indicating which of the document data is used to generate the document signature;
a verification section for receiving the hardcopy document having the document data thereon, the document signature, and the associated data indicator, and performing a comparison to determine whether the document signature was generated using the signor key and the document data indicated by the data indicator; and
an output section for outputting an indication, based on the results of the comparison, of whether the document signature was generated using the signor key and the

document data indicated by the data indicator.

[c2] The system of Claim 1, wherein the comparison is between the document signature and a verification signature generated using a verification key to encode data selected according to the data indicator from the document data on the received hardcopy document.

[c3] The system of Claim 2, wherein the signor key and verification key are substantially identical and the encoding of the document data is performed using a symmetric cryptosystem such as DES.

[c4] The system of Claim 3, wherein the document signature is formed from a portion of a full signature generated using the signor key to encode data selected from the document data and the verification signature is formed from a portion of a full signature generated using the verification key to encode data selected from the document data.

[c5] The system of Claim 1, wherein the comparison is between data selected according to the data indicator from document data on the received hardcopy document and data recovered from the document signature using a verification key.

[c6] The system of Claim 5, wherein the signor key and veri-

fication key are substantially identical and the encoding of the document data and recovery of the data from the document signature are performed using a symmetric cryptosystem such as DES.

[c7] The system of Claim 5, wherein the signor key is a private key and the verification key is a public key and the encoding of the document data and recovery of the data from the document signature is performed using an asymmetric cryptosystem such as RSA.

[c8] The system of Claim 1, wherein the document data required to be written on the hardcopy document includes a document identification number which is combined with the signor key to generate the document signature.

[c9] The system of Claim 1, wherein the hardcopy document is a check.

[c10] The system of Claim 9, further comprising a bearer indicator associated with the check indicating whether or not the bearer of the hardcopy document, who is not the payee, is allowed to clear the check.

[c11] The system of Claim 9, wherein the document data required to be written on the check includes a check identification number which is combined with the signor key to generate the document signature.

[c12] The system of Claim 11, wherein the document data required to be written on the check and which is combined with the signor key to generate the document signature additionally includes data selected from the set consisting of: a check amount, a check date, a payee name, a signor account number and a bank routing number.

[c13] The system of Claim 12, wherein the data indicator printed on the check indicates which of the check amount, check date and payee name are used to generate the document signature.

[c14] The system of Claim 1, further comprising at least one printer for printing the document signature and wherein the document signature is associated with the hardcopy document by placing the printed signature on the hardcopy document.

[c15] The system of Claim 1, wherein the document signature is comprised of a series of characters.

[c16] The system of Claim 15, wherein at least one of the document signature characters is the data indicator indicating which of the document data is used to generate the signature.

[c17] The system of Claim 1, further comprising a portable

hand-carryable housing enclosing:
a memory storage device for storing the signor key;
an input device for receiving the document data and storing it in the memory storage device;
a processor for retrieving the signor key and document data from the memory storage and generating the document signature by encoding the document data using the signor key; and
an output device for outputting the document signature.

[c18] The system of Claim 17, further comprising a biometric sensor connected to the housing and providing biometric information of the signor for accessing the signor key.

[c19] The system of Claim 17, wherein the output device is a printer.

[c20] The system of Claim 17, wherein the input device allows the signor to manually input at least a portion of the document data.

[c21] The system of Claim 1, wherein the document signature is associated with the hardcopy document by marking the document signature on the document and the verification section reads the associated signature on the hardcopy document using optical mark recognition.

[c22] The system of Claim 1, wherein the signature is associ-

ated with the hardcopy document by printing the signature on a sticker and sticking the sticker on the document.

[c23] The system of Claim 1, wherein the signor manually inputs into the system the document data required to be written on the hardcopy document, the system further comprising a printer for printing the document data and the signature directly on the hardcopy document.

[c24] The system of Claim 1, wherein the system displays the document signature and the signor manually writes characters forming the displayed document signature onto the hardcopy document.

[c25] The system of Claim 9, wherein the verification section comprises:
a payee bank for receiving the check having the associated signature; and
an inter-bank connection for forwarding the document data and information contained in the document signature to a bank computer system for determining whether the signature was generated using the signor key and the document data to thereby verify the document signature.

[c26] The system of Claim 9, wherein the verification section

comprises:

an automated teller machine for receiving the check and reading the document data and document signature associated therewith; and

a connection for forwarding the read document data and document signature to a bank computer system for determining whether the document signature was generated using the signor key and the document data to thereby verify the document signature.

[c27] The system of Claim 9, wherein the verification section comprises:

an Internet banking system for acquiring the document data and document signature associated therewith and for forwarding the document data and document signature to a bank computer system for determining whether the signature was generated using the signor key and the document data to thereby verify the document signature.

[c28] The system of Claim 9, wherein the verification section comprises:

a telephone banking system for acquiring the document data and document signature associated therewith and for forwarding the document data and signature to a bank host computer system for determining whether the document signature was generated using the signor key

and the document data to thereby verify the document signature.

[c29] The system of Claim 9, wherein the verification section comprises:
a payee section located at the location of a payee of the check for acquiring the document data and document signature with the check and for forwarding the document data and signature to a bank host computer system for determining whether the signature was generated using the signor key and the document data to thereby verify the document signature.

[c30] The system of Claim 1, wherein access to the signor key is controlled using biometric information of the signor.

[c31] The system of Claim 1, wherein the document is a fund transfer form used to transfer money.

[c32] The system of Claim 9, wherein the verification section comprises: a mobile banking system for acquiring the document data and document signature and for forwarding the document data and document signature to a bank computer system for determining whether the signature was generated using the signor key and the document data to thereby verify the document signature.

[c33] The system of Claim 1, wherein the signature generation

part includes first and second signature generation parts and wherein:
the first signature generation part generates an intermediate document signature using the signor key to encode data selected from the document data; and
the second signature generation part generates the document signature using a second signor key to encode the intermediate document signature and data indicator.

[c34] The system of Claim 33, wherein the verification section includes:
a decoding section using a verification key to decode the document signature to produce the intermediate document signature and the data indicator;
an encoding section using a second verification key for encoding the document data from the received hardcopy document indicated by the data indicator to generate a verification intermediate document signature; and
a comparison section for performing the comparison by comparing the decoded intermediate document signature to the verification intermediate document signature.

[c35] A method for generating and verifying signatures on hardcopy documents comprising the steps of:
storing a signor key associated with a signor of a hardcopy document;
acquiring document data required to be written on the

hardcopy document;
generating a document signature using the signor key to encode data selected from the document data;
generating a data indicator indicating which of the document data is used to generate the document signature;
associating the document signature and data indicator with the hardcopy document;
receiving for verification the hardcopy document having its associated document signature, data indicator and document data written thereon;
performing a comparison to determine whether the document signature was generated using the signor key and the document data indicated by the data indicator; and
outputting an indication, based on the results of the comparison, of whether the document signature was generated using the signor key and the document data indicated by the data indicator.

[c36] The method of Claim 35, wherein the comparison is between the document signature and a verification signature generated using a verification key to encode data selected according to the data indicator from the document data on the received hardcopy document.

[c37] The method of Claim 36, wherein the signor key and verification key are substantially identical and the encoding of the document data is performed using a symmet-

ric cryptosystem such as DES.

[c38] The method of Claim 37, wherein the document signature is formed from a portion of a full signature generated using the signor key to encode data selected from the document data and the verification signature is formed from a portion of a full signature generated using the verification key to encode data selected from the document data.

[c39] The method of Claim 35, wherein the comparison is between data selected according to the data indicator from document data on the received hardcopy document and data recovered from the document signature using a verification key.

[c40] The method of Claim 39, wherein the signor key and verification key are substantially identical and the encoding of the document data is performed using a symmetric cryptosystem such as DES.

[c41] The method of Claim 39, wherein the signor key is a private key and the verification key is a public key and the encoding of the document data and recovery of the data from the document signature are performed using an asymmetric cryptosystem such as RSA.

[c42] An apparatus for generating and placing digital signa-

tures on checks comprising:

a signor key associated with a signor of the check;

check information required to be written on the check including a check identification number and bank routing number along with information selected from the set consisting of: a check amount, a check date and a payee name;

an encoded signature which is generated by using the signor key to encode data selected from the check information and which is then placed on the check; and

a data indicator indicating which of the check amount, the check date and the payee name are used to generate the signature.